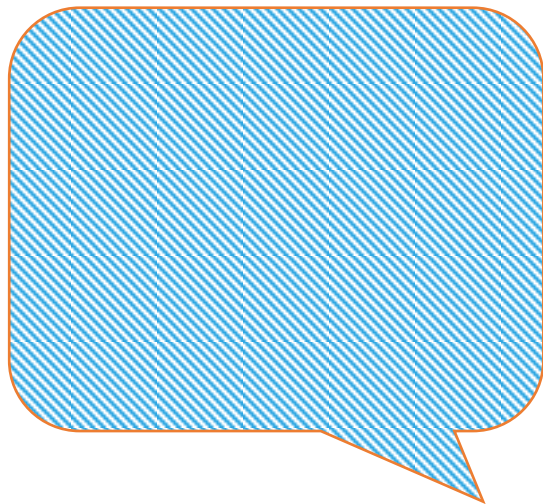




Datos 2016 CCN-CERT

DIEZ AÑOS FORTALECIENDO LA
CIBERSEGURIDAD NACIONAL



- Javier Candau
- Centro Criptológico Nacional
- ccn@cni.es

Índice

- 1. Cambios Legislativos**
- 2. Formación e información**
- 3. Sistemas de Alerta**
- 4. Otras herramientas**
- 5. Intercambio**
- 6. Cumplimiento objetivos 2016 / 2017**

CAMBIOS LEGISLATIVOS

Publicación / entrada en vigor

Ley 39 y 40 / 2015 (en vigor desde 01.10.2016)

- CCN-STIC 830 Ámbito de aplicación del Esquema Nacional de Seguridad
- RD 951/2015 (Nuevo PLAN ADECUACIÓN al ENS) (en vigor el 4.11.2017)

REGLAMENTO (UE) 2016/679 de 27 de abril de 2016. Tratamiento y libre circulación de datos personales

DIRECTIVA (UE) 2016/1148 de 06 de julio de 2016. (NIS) Medidas para garantizar un nivel común de seguridad en redes y sistemas



2016...

23 cursos
2454 solicitudes
670 alumnos
995 horas lectivas

PLAN DE FORMACIÓN



10 cursos

XIII Curso STIC
XI Curso Básico STIC Infraestructura Red
IX Curso STIC Búsqueda Evidencias
VIII Curso STIC Seguridad App Web
XI Curso STIC Inspecciones Seguridad
XIII Curso STIC Acreditación Windows
XI Curso Básico STIC BBDD
XXVII Curso Especialidades Criptológicas
I Curso STIC Gestión Incidentes
XIII Curso Gestión STIC
XII Curso STIC Detección Intrusos (IDS)
XI Curso STIC Seg. Redes Inalámbricas
VII Curso STIC Herramienta PILAR
V Curso STIC Dispositivos Móviles
II Curso STIC Gestión Incidentes

Curso STIC Ad Hoc para la DGP
Curso STIC Ad Hoc para el ET
Curso STIC Ad Hoc México
Curso CEC Ad Hoc Perú
Curso online Ad Hoc Windows Armada
Curso Acreditación Empresas (ONS)
Sesión teleformación INES
Sesión teleformación ENS

PLAN DE FORMACIÓN



Centro Criptológico Nacional 2017

	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	
ENE																															
FEB																															
MAR																															
ABR																															
MAY																															
JUN																															
JUL																															
AGO																															
SEP																															
OCT																															
NOV																															
DIC																															

PLAN DE FORMACIÓN



10 cursos



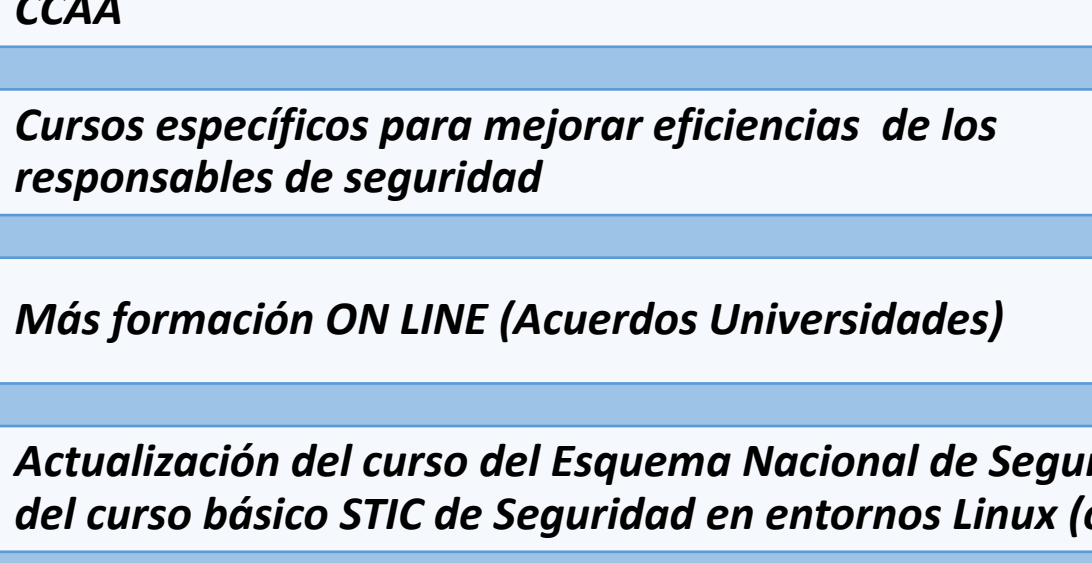
Centro Criptológico Nacional

2017

DE FORMACIÓN

	L	M	X	J	V	S	D	L	M	X	J	V	S	D	L	M	X	J	V	S	D
ENE							1	2	3	4	5	6	7	8	9	10	11	12			
FEB							1	2	3	4	5	6	7	8	9	10	11	12			
MAR							1	2	3	4	5	6	7	8	9	10	11	12			
ABR							1	2	3	4	5	6	7	8	9	10	11	12			
MAY							1	2	3	4	5	6	7	8	9	10	11	12			
JUN							1	2	3	4	5	6	7	8	9	10	11	12			
JUL							1	2	3	4	5	6	7	8	9	10	11	12			
AGO							1	2	3	4	5	6	7	8	9	10	11	12			
SEP							1	2	3	4	5	6	7	8	9	10	11	12			
OCT							1	2	3	4	5	6	7	8	9	10	11	12			
NOV							1	2	3	4	5	6	7	8	9	10	11	12			
DIC							1	2	3	4	5	6	7	8	9	10	11	12			

Objetivos 2017:

- 
- The infographic consists of a vertical blue bar on the left with white numbers 1 through 5. To the right of the bar are five horizontal white boxes with blue borders, each containing a measure. The measures are listed in bold black text.
- 1 • ***Aumentar la oferta de formación a distancia para EELL y CCAA***
 - 2 • ***Cursos específicos para mejorar eficiencias de los responsables de seguridad***
 - 3 • ***Más formación ON LINE (Acuerdos Universidades)***
 - 4 • ***Actualización del curso del Esquema Nacional de Seguridad y del curso básico STIC de Seguridad en entornos Linux (online)***
 - 5 • ***1 Curso Avanzado Gestión Incidentes de Ciberseguridad***

269 guías
366 documentos

2015

23 nuevas guías
5 actualizadas

2016

19 nuevas guías
12 actualizadas

Listado de Guías CCN-STIC



14 de noviembre de 2014

Guía CCN-STIC
461

Guía CCN-STIC
462

Guía CCN-STIC
830

Guía CCN-STIC
845

Guía CCN-STIC
599

Guía CCN-STIC
899

Guía CCN-STIC
001

Guía CCN-STIC
101

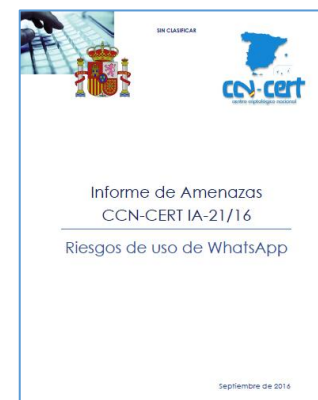
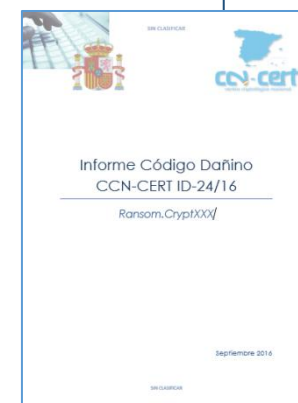


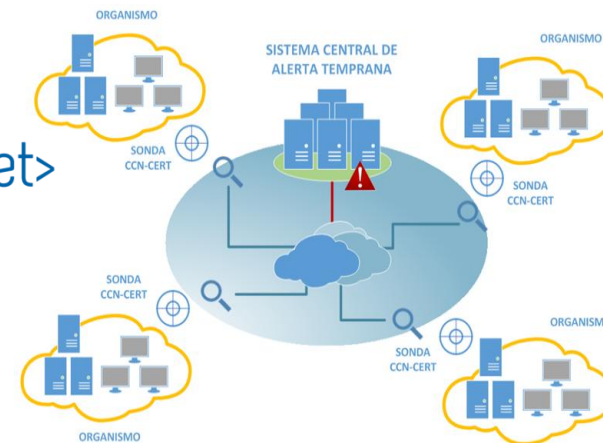
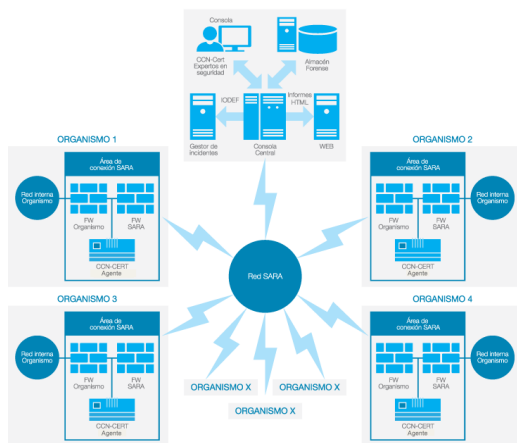
www.ccn-cert.cni.es

INFORMACIÓN (GUÍAS e INFORMES)

117

Informes de Amenazas (IA) (30)
Informes de Código Dañino (ID) (27)
Informes Técnicos (IT) (56)
Buenas Prácticas (BP) (4)





- Servicio por suscripción
- Basado en despliegue de sondas.
- **108 Organismos**
- **129 sondas**
- + 90 millones eventos
- + 17.000 incidentes

PortalSAT-SARA: Examinar ...

https://portalsat-sara-dev.redsara.es/informes/flow.html?_flowId=searchFlow

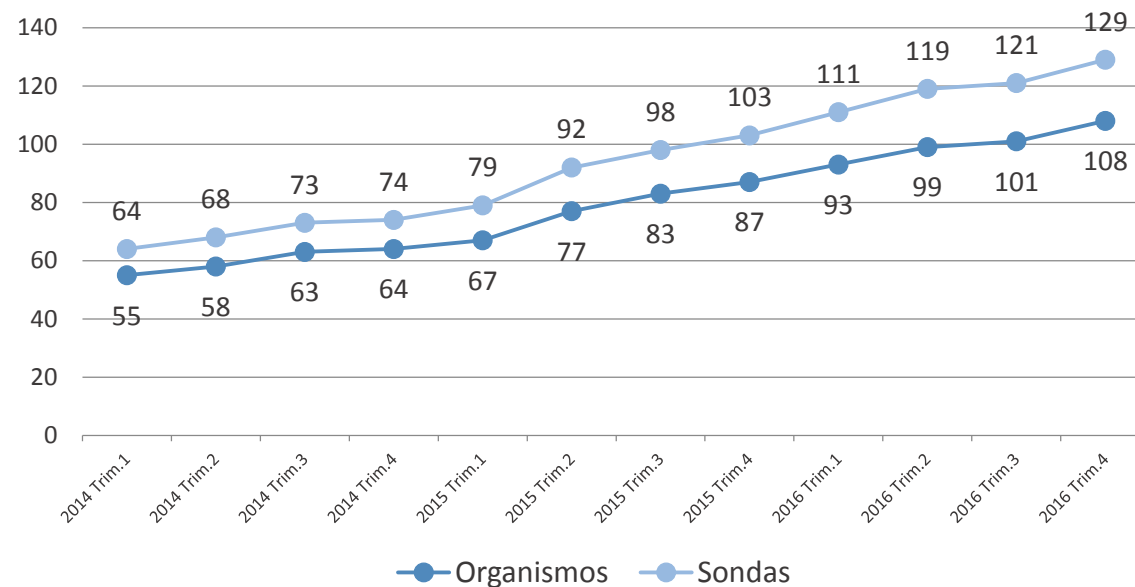
Más visitados Comenzar a usar Firefox infoSARA Inicio de ses...

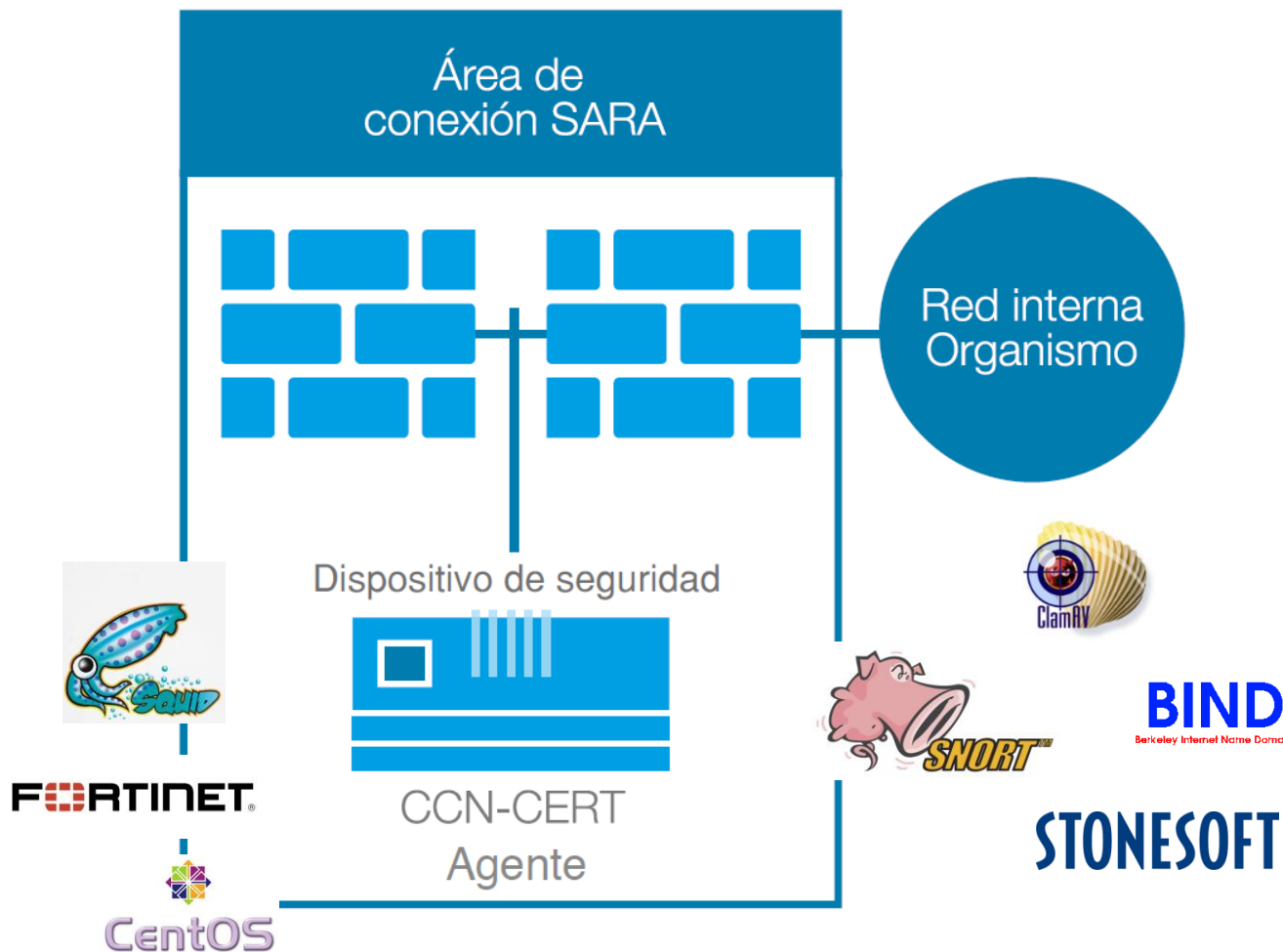
SISTEMA DE ALERTA TEMPRANA DE LA RED SARA

SAT SARA Biblioteca Ver andalucia

Ordenación por: Nombre Fecha modificada

Nombre	Descripción	Tipo	Fecha de c...	Fecha modi...
InformeMensual-ANDALUCIA-201602.p...	Recurso de conter julio 20		julio 20	
InformeMensual-ANDALUCIA-201603.p...	Recurso de conter julio 27		julio 27	
InformeMensual-ANDALUCIA-201604.p...	Recurso de conter julio 20		julio 20	
InformeMensual-ANDALUCIA-201606.p...	Recurso de conter junio 22		junio 22	
InformeMensual-ANDALUCIA-201607.p...	Recurso de conter julio 20		julio 20	
InformeMensual-ANDALUCIA-201608.p...	Recurso de conter agosto 12		agosto 12	



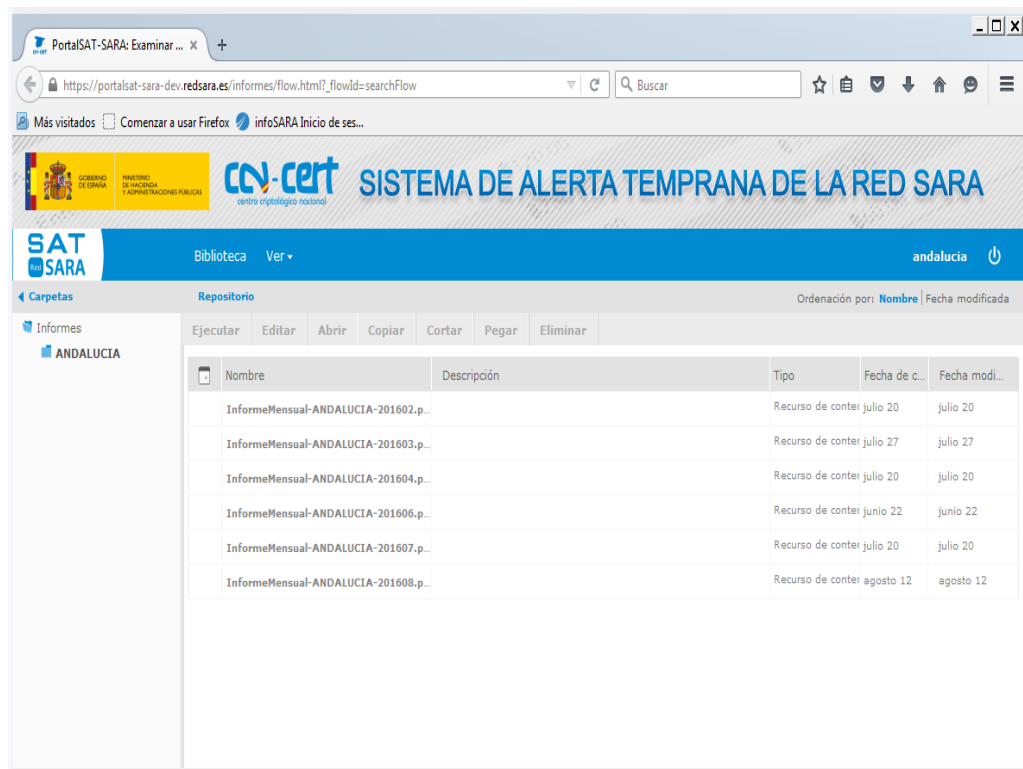


- Conjunto de AAPP
- Varias fuentes análisis
- **50 sondas** desplegadas

+40% incidentes
notificados (respecto 2015)



➤ Portal de informes



➤ Servicio de Análisis de Vulnerabilidades



SERVICIO DE ANÁLISIS DE VULNERABILIDADES

Sistema de Alerta Temprana
de la red SARA





AGE

53 organismos
65 sondas
835.000 usuarios



CCAA

13 organismos
15 sondas
227.000 usuarios



EELL

14 organismos (+2)
15 sondas
112.000 usuarios



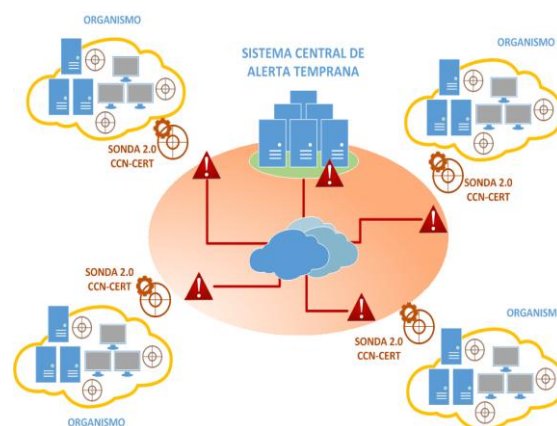
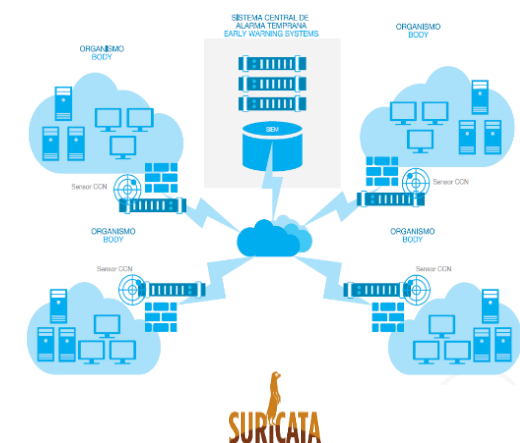
Universidades

10 organismos
10 sondas
35.000 usuarios

V1.0

2016

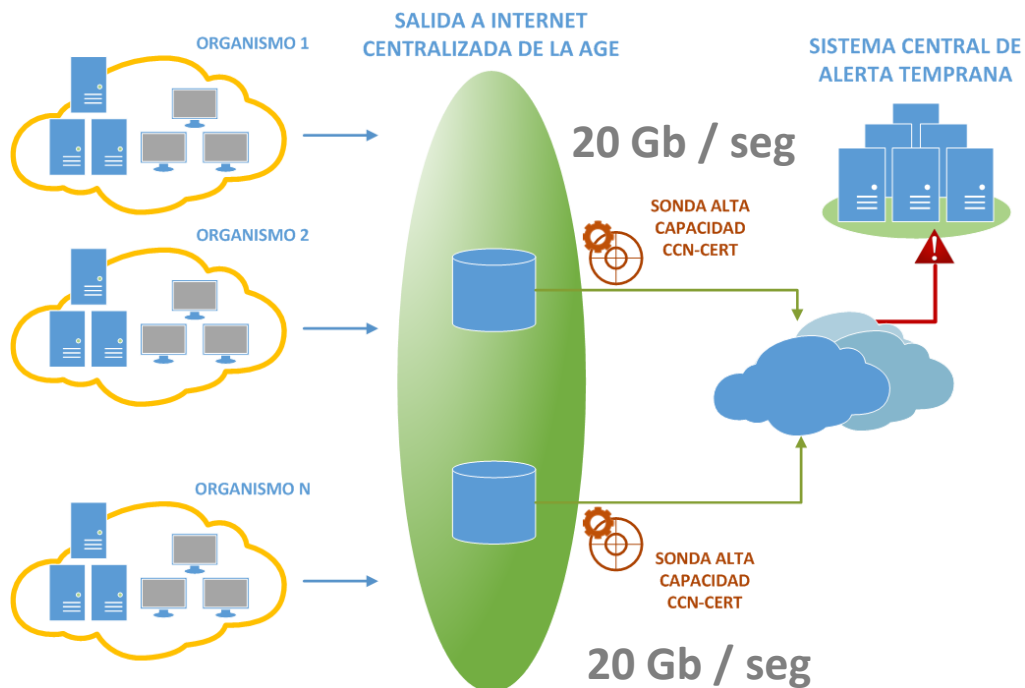
V2.0



- › Multinivel
- › **30 sensores** desplegados
- › Nuevo motor de correlación
- › Nuevas fuentes de información

SECTOR PÚBLICO

18 EMPRESAS
ESTRATEGICAS



SONDA AGE

Organismos que pertenecen al SAT de Internet



21



Organismos que no pertenecen al SAT de Internet

23



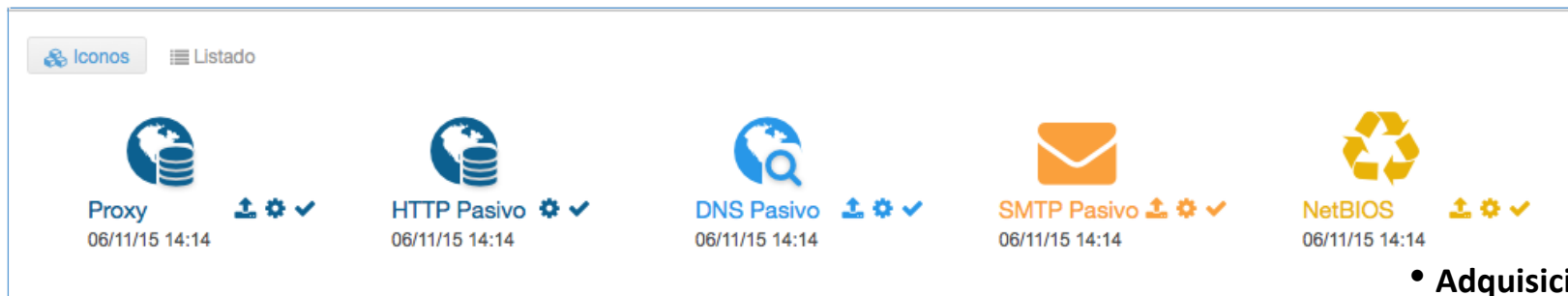
- Despliegue de dos sondas en los dos puntos de agregación (solución de Verint)
 - ♦ Sondas en Tecnoalcalá (Telefónica) y en el CPD del MEYSS.
 - ♦ Envío de eventos al **Sistema Central del SAT de Internet**.
 - ♦ Servicio a organismos que no están en el SAT actualmente.

SAT Sistemas Control Industrial

1. **Mínima intrusión** en el sistema monitorizado. La concepción es la de un sistema de alerta, sin bloquear en ningún caso ni restringir la operación del mismo.
2. Detección de acciones anómalas contra los procesos industriales basadas en el análisis del contexto.
3. Disectores específicos de protocolos industriales y motor de correlación local.
 - **EthernetIP (ya desarrollado y probado)**
 - **S7Com (Siemens)**
 - **FINS (Omron)**
 - **Modbus TCP (Estándar)**



SECTOR PÚBLICO



CARMEN



➤ Permite el **estudio estadístico / basado en conocimiento** del tráfico:

- HTTP
- DNS
- SMTP
- NetBIOS

➤ Puede capturar **tráfico en vivo**, analizar **logs de proxy** o cargar tráfico a partir de **pcaps**.

➤ **45 incidentes de criticidad > alto** detectados en 2016

➤ **24 appliances** desplegados

➤ **9 appliances** en proceso de despliegue

carmen

5.0

• Adquisición

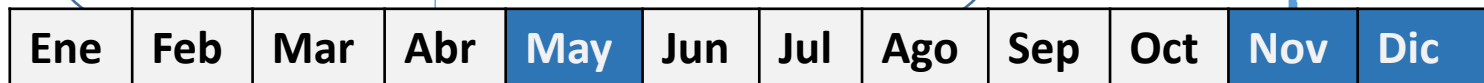
Certificados HTTPS
Integración Bot Killer
Cookies HTTP

• Investigaciones

Informe de investigaciones

• Mejoras en el interfaz

Mejora en la gestión de
listas en eventos



carmen

5.2

Previsto: 30/12/16

• Interoperabilidad

Integración con LUCIA
Integración con REYES
Integración con eMas

• Investigaciones

Múltiples investigaciones
abiertas

• Mejoras en el interfaz

Agrupación por Referer

• Puesto de usuario

Windows Carmen Agent

HERRAMIENTAS

DETECCIÓN



SONDA AGE

ANÁLISIS



AUDITORÍA



CLAUDIA

INTERCAMBIO



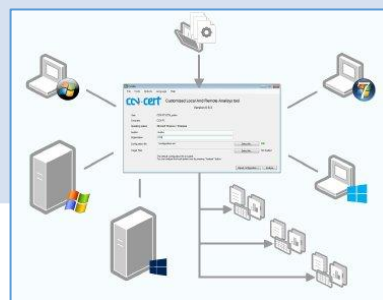
HERRAMIENTAS DE AUDITORÍA (I)



- Versión 6.2
- MicroPILAR Protección Datos
- MicroPILAR Infraestructuras Críticas
- Integración con INES 
- Integración con CLARA 
- Integración con ROCIO
- Apoyo a Documentación Seguridad Sistemas Clasificados

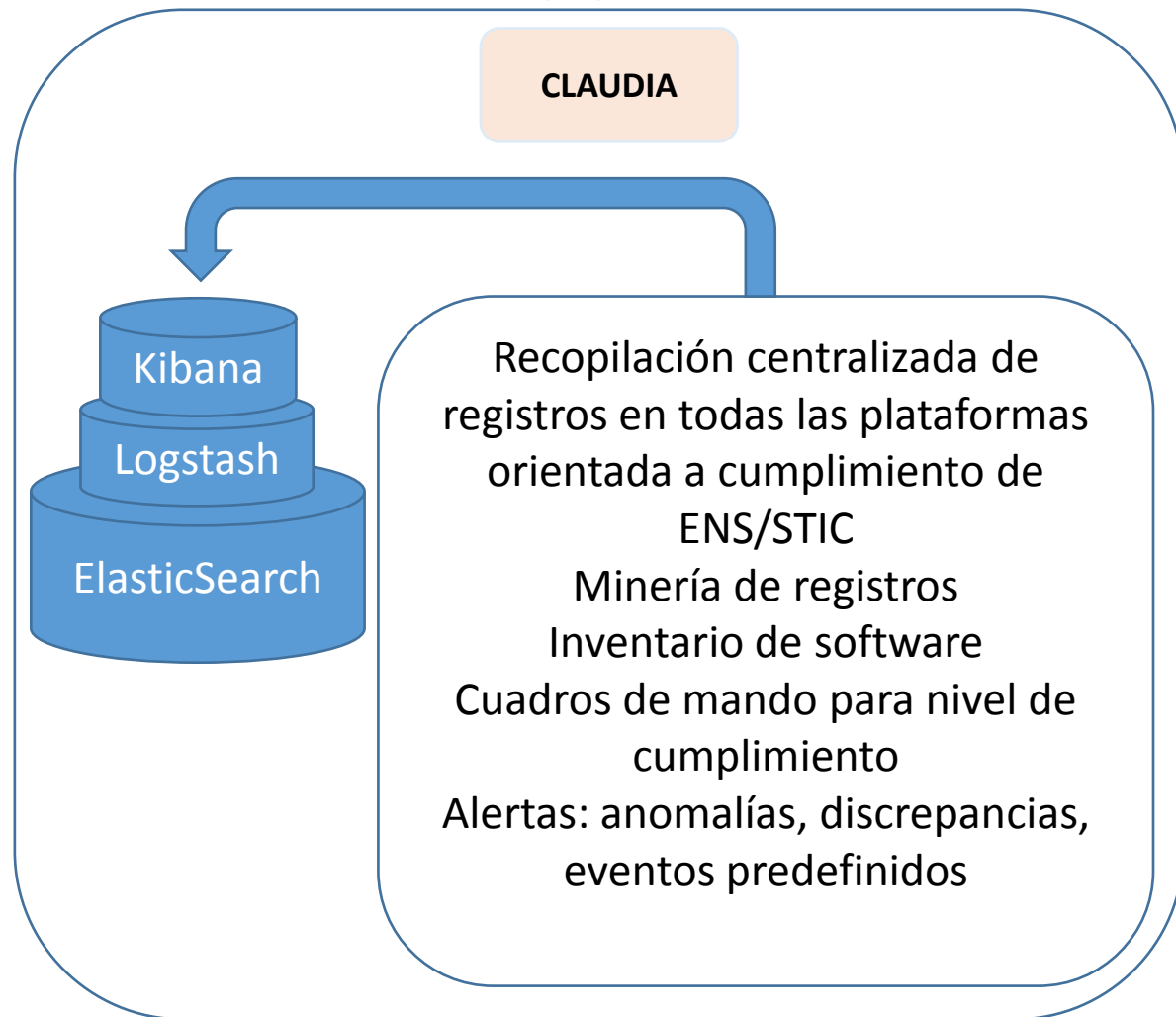
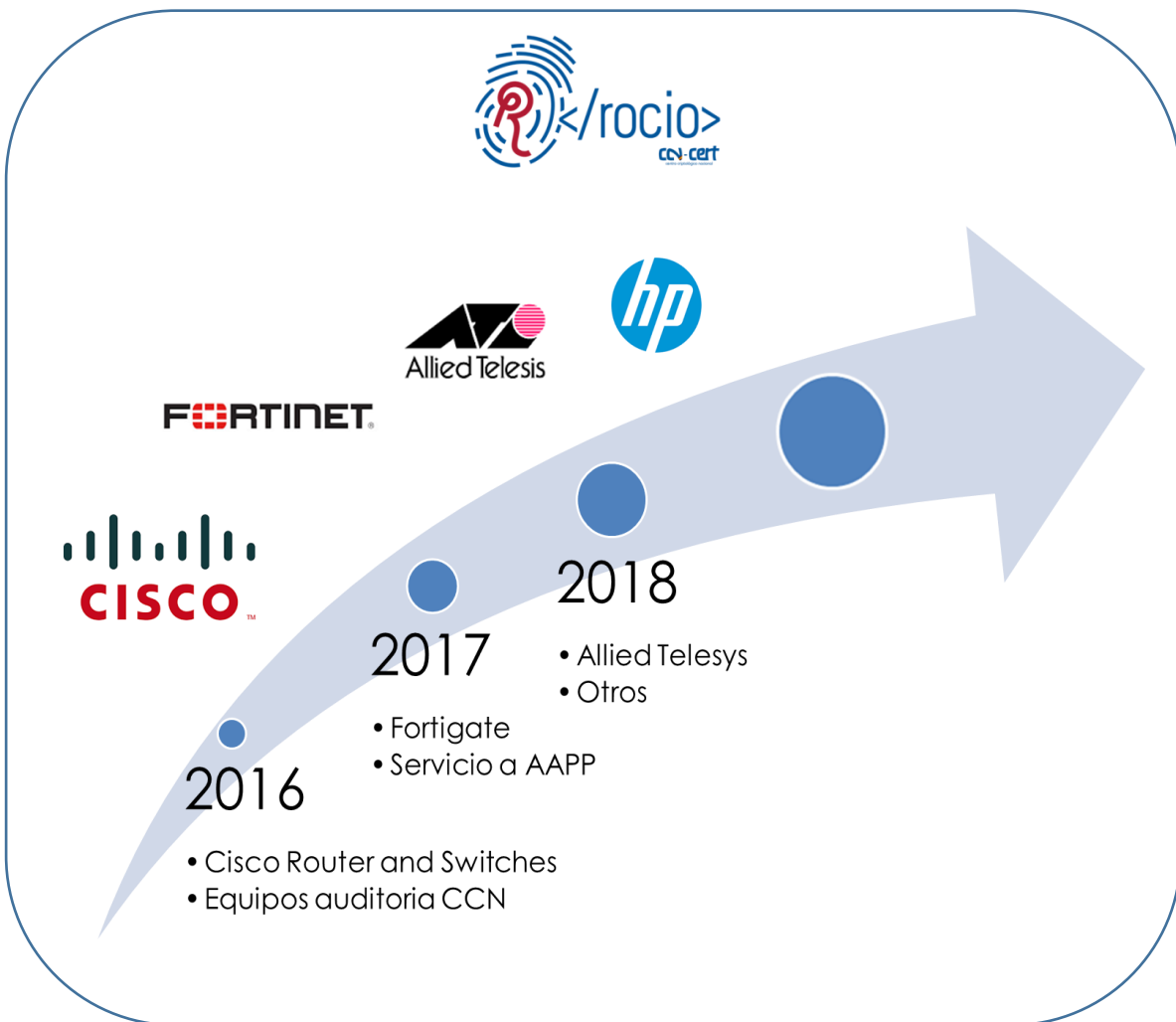


- Modelo distribuido
- Análisis de WINDOWS 10
- Valoración continua del nivel de seguridad de los sistemas
- Aplicación de las CCN-STIC
- Apoyo a la configuración de Seguridad Sistemas Clasificados

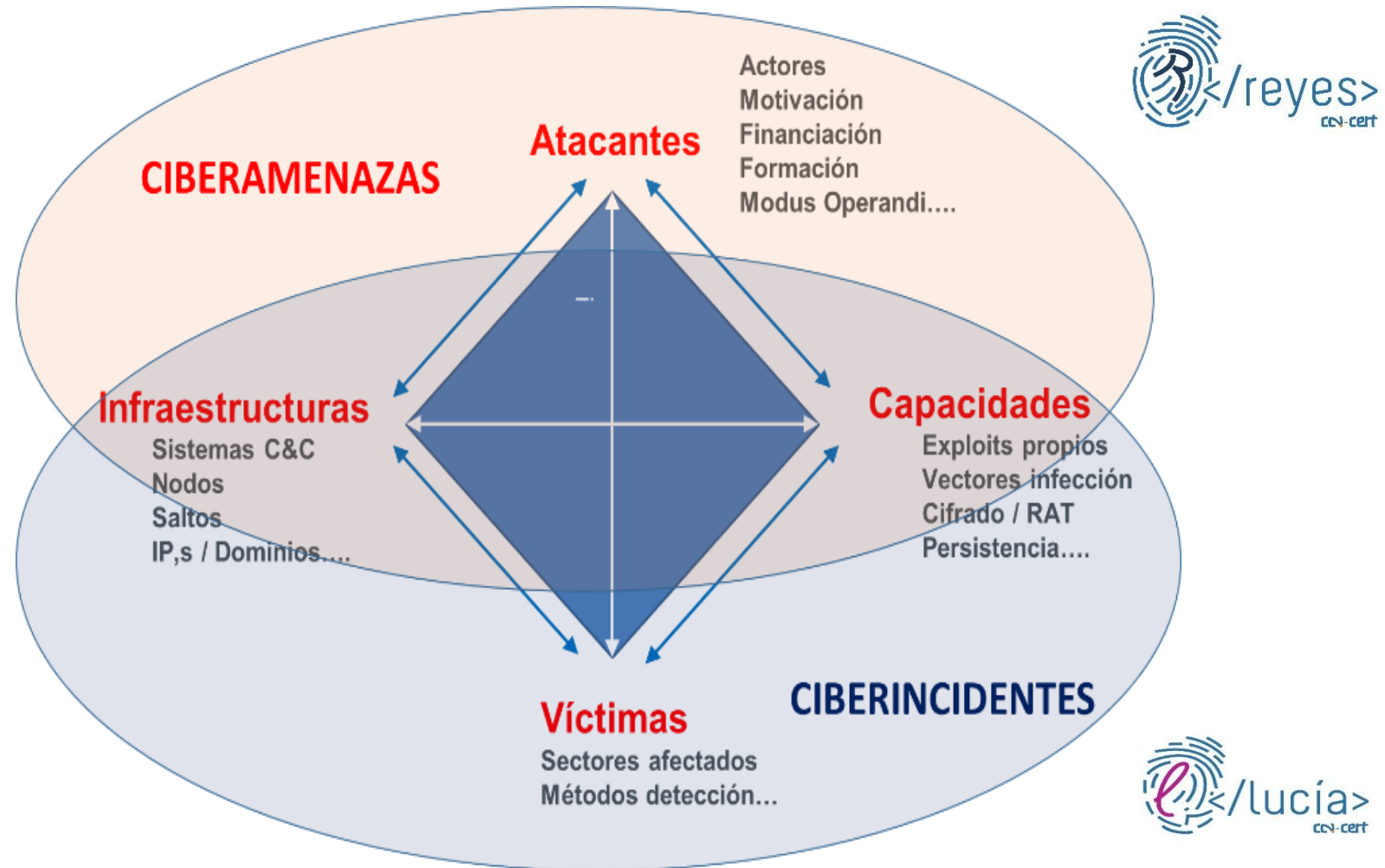


- Análisis de equipos de comunicaciones
 - Conexiones
 - Firmware y sistema operativo
 - Configuración
- Apoyo a la configuración de Seguridad Sistemas Clasificados
- rocio@ccn-cert.cni.es

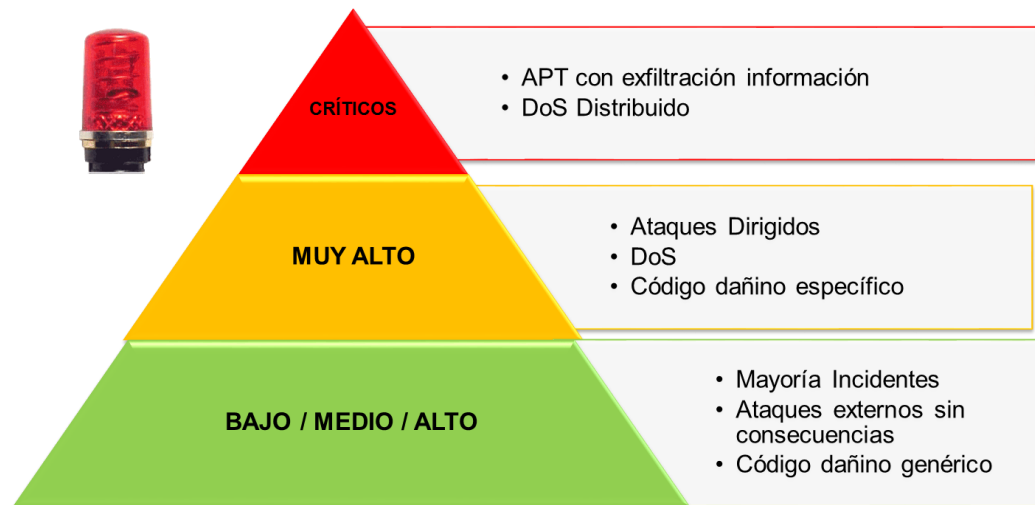
HERRAMIENTAS DE AUDITORÍA (II)



INTERCAMBIO Y CONOCIMIENTO DE LA AMENAZA



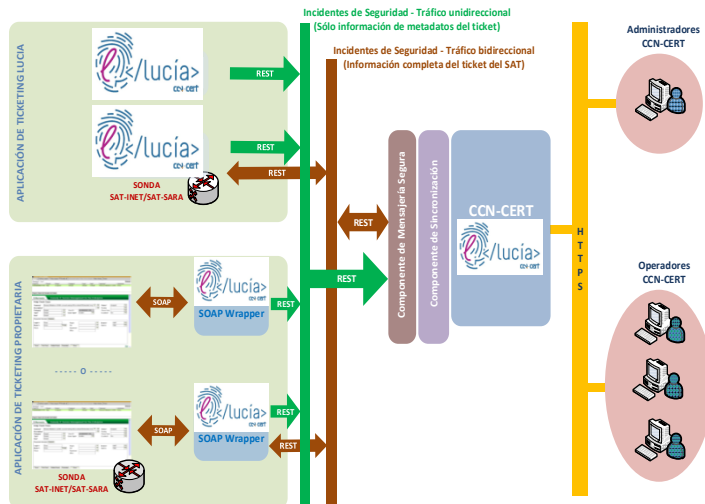
CLASIFICACIÓN DE LOS INCIDENTES



Guía CCN-STIC-817– Criterios Comunes y Gestión de Incidentes

OBLIGACIÓN DE NOTIFICAR:

- RD 3/2010 que regula el Esquema Nacional de Seguridad (ENS)
- Ley 8/2011 - RD 704/2011 Protección de las Infraestructuras Críticas (Instrucciones de la SES para IC) .
- REGLAMENTO (UE) 2016/679 de 27.04.2016. Tratamiento y libre circulación **datos personales** .
- DIRECTIVA (UE) 2016/1148 de 06.07.2016. **(NIS)**. Servicios esenciales (Seg. Redes y sistemas)



LUCIA



15 Organismos federados
7 Organismos federándose
+90 LUCIA central

Resolución

Resolución: (sin valor)

Recursos Invertidos: (sin valor)

Categoría del Sistema según ENS: (sin valor)

Impacto: (sin valor)

Causa del Incidente: Seleccionar valores múltiples

- ☐ C.10 - Configuración inadecuada
- ☐ C.11 - Ausencia o deficiencia de mantenimiento
- ☐ C.12 - Inadecuada ejecución de un cambio
- ☐ C.13 - Falta de concienciación del personal
- ☐ C.14 - Deficiente formación del personal
- ☐ II.05 - Han requerido el sistema de protección frente a incendios y éste ha fallado
- ☐ II.06 - Han requerido el sistema de protección frente a inundaciones y éste ha fallado
- ☐ II.91 - Ha sido necesario recurrir a las instalaciones alternativas y éstas no han funcionado según el plan previsto
- ☐ II.92 - Ha sido necesario recurrir a personal alternativo y esto no ha funcionado según el plan previsto
- ☐ II.93 - Ha sido necesario recurrir al equipamiento alternativo y éste no ha funcionado según el plan previsto

Incidencias durante la Resolución: Seleccionar valores múltiples

Número de Sistemas Afectados: (sin valor)

¿Afecta a la LOPD?: (sin valor)

¿Afecta a la LPIC? (Ley 8/2011): (sin valor)

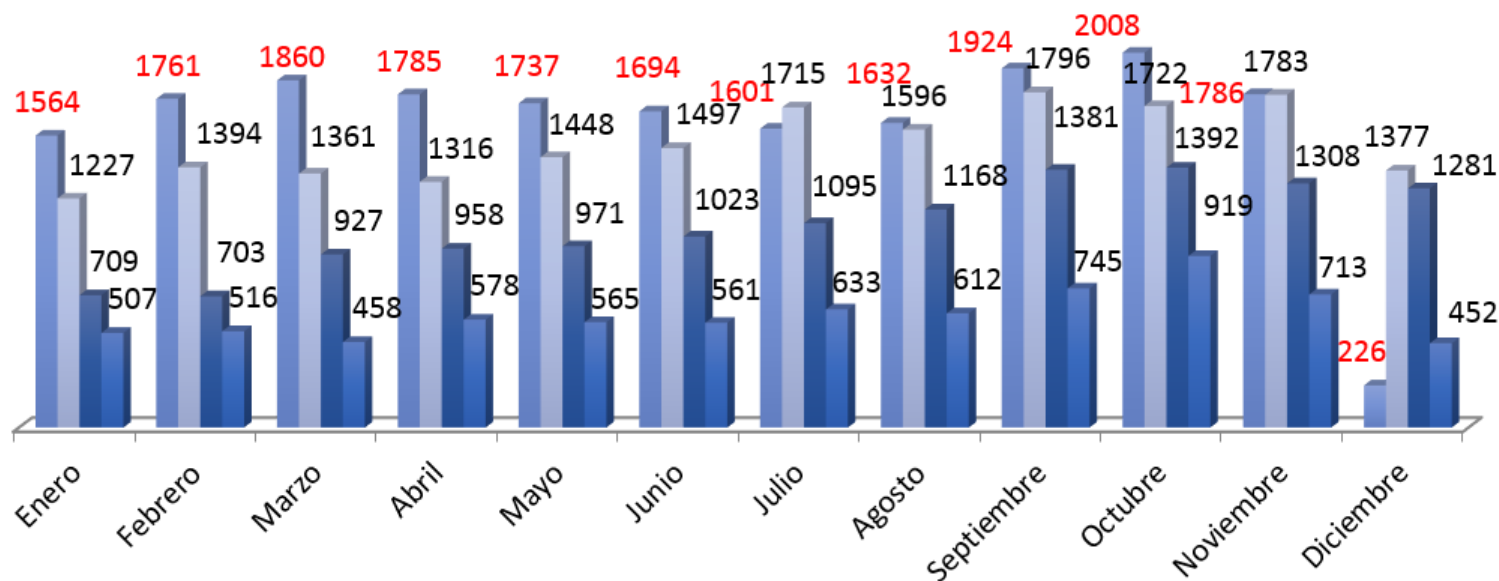
Tiempo Trabajado: Minutos

ESTADÍSTICAS DE INCIDENTES CON LUCIA (+800 procedentes de LUCIA federados)

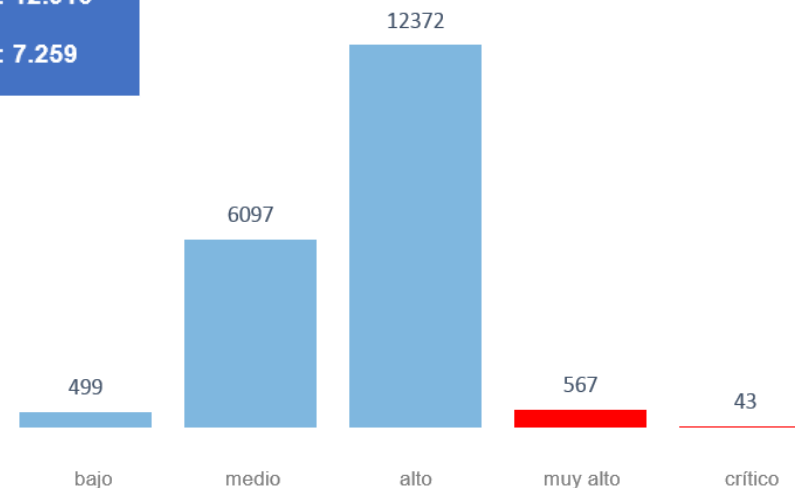
■ 2016 ■ 2015 ■ 2014 ■ 2013

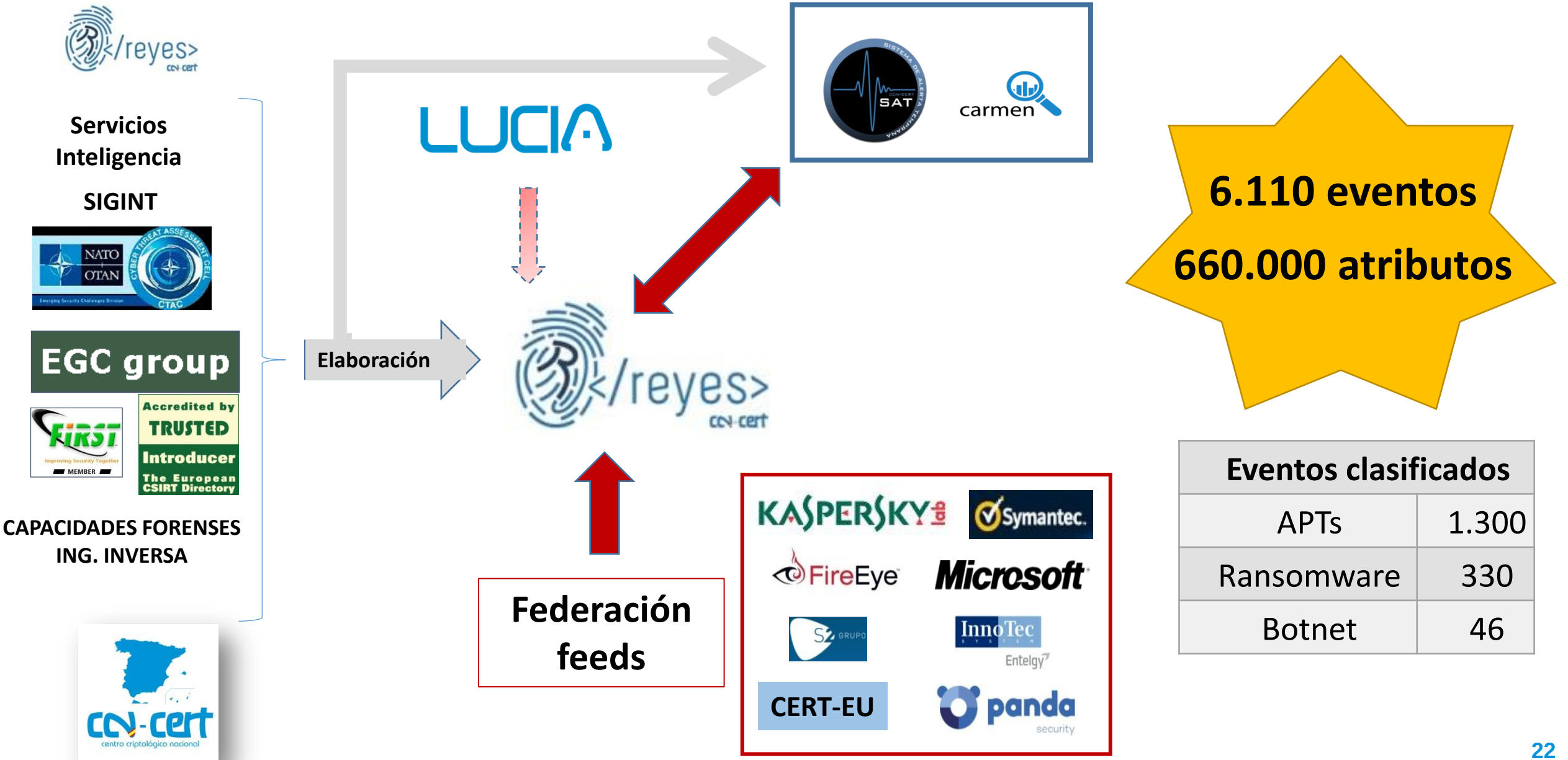
+27%	+27%	+37%	+36%	+20%	+13%	-7%	+2%	+7%	+17%	+0%
------	------	------	------	------	------	-----	-----	-----	------	-----

a 05.12.2016



Acumulado Anual
2016: 19.578
2015: 18.232
2014: 12.916
2013: 7.259





INFORMES DE INTELIGENCIA

+ 2.000 informes sobre APT

FireEye THREAT INTELLIGENCE

Microsoft Windows Escalation Exploited in Conjunction with Flash Player Vulnerability Activity

Fusion (FS)

Vulnerability and Exploitation (VE)

November 07, 2016 12:58:00 PM, 16-00017374

Executive Summary

- Microsoft confirmed the existence of a Windows kernel escalation of privilege (EoP) vulnerability (16-00017148) being exploited in the wild in conjunction with the recently patched Flash Player vulnerability (CVE-2016-7855 (16-00016766)).
- Microsoft has attributed the use of this vulnerability to the Tsar Team.
- Microsoft has stated that they plan to release a patch for the EoP vulnerability.

Threat Detail

Microsoft Confirms Existence of Windows Escalation of Privilege (EoP) Vulnerability

Microsoft has publicly confirmed that Adobe Flash Player was exploited in conjunction with a Windows kernel escalation of privilege (EoP) vulnerability, limiting the need for victim

KAISERCKV

Expert analysis:
Guccifer2.0 unlikely to be Romanian

Version: 1.0 (23 June 2016)

Distribution: this document is TLP: AMBER. For more information on TLP: AMBER, see <https://www.us-cert.gov/tlp>

On June 14, 2016 The Washington Post¹ published how "Russian government Democratic National Committee (DNC) network for more than 2 years. The source was a blogpost from CrowdStrike² detailing how they found samples from CrowdStrike's Incident Response investigation for the DNC.

On June 15, a "lone hacker" calling himself Guccifer2.0, claimed responsibility for the hack and showed some documents as a proof of the hack and against CrowdStrike's analysis:

"Shame on CrowdStrike: Do you think I've been in the DNC's networks for almost 2 years? Do you really believe it?"

The "original" Guccifer (not to be confused with Guccifer2.0) is a Romanian hacker who was responsible for hacking the e-mail accounts of many celebrities and currently awaiting for sentencing, after being extradited by Romania to the United States.

On June 21, 2016, Motherboard³ published an interview with Guccifer2.0. The hacker declared again he is from Romania.

DeepSight™ INTELLIGENCE

SWALLOWTAIL COMPROMISE

MANAGED AND MONITORED

DEEPSIGHT™ INTELLIGENCE

SIN CLASIFICAR

CCN-CERT
centro criptológico nacional

Informe Código Dañino
CCN-CERT ID-16/16

"Volgmer"

OBJETIVOS 2016 / 2017

1. SAT SARA (despliegue portal informes / análisis vulnerabilidades)
2. SAT Internet 2.0 (finalizar despliegue) 
3. Monitorización salida agregada (decisión herramienta a utilizar)
4. ENS. Mejora y precisión en el conocimiento del nivel de seguridad.
 - Impulsar las certificaciones de cumplimiento.
5. REYES / LUCIA. Intercambio real de amenazas / incidentes 
6. Formación online. Curso gestión incidentes (avanzado) (Formación a distancia) 
7. Productos / Organismo de Certificación (CATÁLOGO) 
8. Seguimiento de incidentes con equipos dedicados / sectoriales 
9. Incrementar la actividad de Auditoría / Inspección (+ herramientas)
10. SAT Control Industrial

19 GUÍAS NUEVAS DESARROLLADAS EN 2016

400 Guías generales	Publicado
CCN-STIC-461 Seguridad en DRUPAL	Jun 2016
CCN-STIC-462 Seguridad en JOOMLA	Ago 2016
CCN-STIC-495 Seguridad en IP v6	Jul 2016

500 Guías de entornos Windows	Publicado
CCN-STIC-515 Servidor de impresión (Windows 2008 Server R2)	Feb 2016
CCN-STIC-552 Exchange server 2013 (Windows Server 2012)	Nov 2016
CCN-STIC-561 Servidor de impresión (Windows Server 2012)	Mar 2016
CCN-STIC-562 Servidor de ficheros (Windows Server 2012)	Sep 2016
CCN-STIC-563 Internet Information Services (8.5 Windows Server 2012)	Nov 2016
CCN-STIC-595 Entidad de certificación (Windows Server 2008)	Mar 2016
CCN-STIC-596 Protección sistema con APPLOCKER	Feb 2016
CCN-STIC-599A Configuración segura Windows 10 (cliente en dominio)	Jul 2016
CCN-STIC-599B Configuración segura Windows 10 (cliente independiente)	Jul 2016

600 Guías otros entornos	Publicado
CCN-STIC-647 Seguridad en switches HP COMWARE	Ene 2016

800 Guías Esquema Nacional de Seguridad	Publicado
CCN-STIC-830 Ámbito aplicación del ENS	Sep 2016
CCN-STIC-873 Implantación ENS en IIS 8.5	Nov 2016
CCN-STIC-880 Implantación del ENS en Exchange Server 2013	Nov 2016
CCN-STIC-899 A Implantación ENS en Windows 10 (cliente en dominio)	Nov 2016
CCN-STIC-899 B Implantación ENS en Windows 10 (cliente independiente)	Nov 2016

900 Informes Técnicos	Publicado
CCN-STIC- 955B Recomendaciones de empleo de GPG	Dic 2016

**2015: 23 nuevas guías
5 actualizadas**

**2016: 19 nuevas guías
12 actualizadas**

12 GUÍAS ACTUALIZADAS DESARROLLADAS EN 2016

000 Políticas	Publicado
CCN-STIC-001 Seguridad de las TIC que manejan información nacional clasificada en la Administración	Jun 2016

100 / 200 / 300 Procedimientos / Normas / Inst. Técnicas	Publicado
CCN-STIC-101 Acreditación Sistemas TIC para manejar información clasificada nacional	Jul 2016
CCN-STIC-103 Catálogo Productos con Certificación Criptológica (DL)	Jun 2016

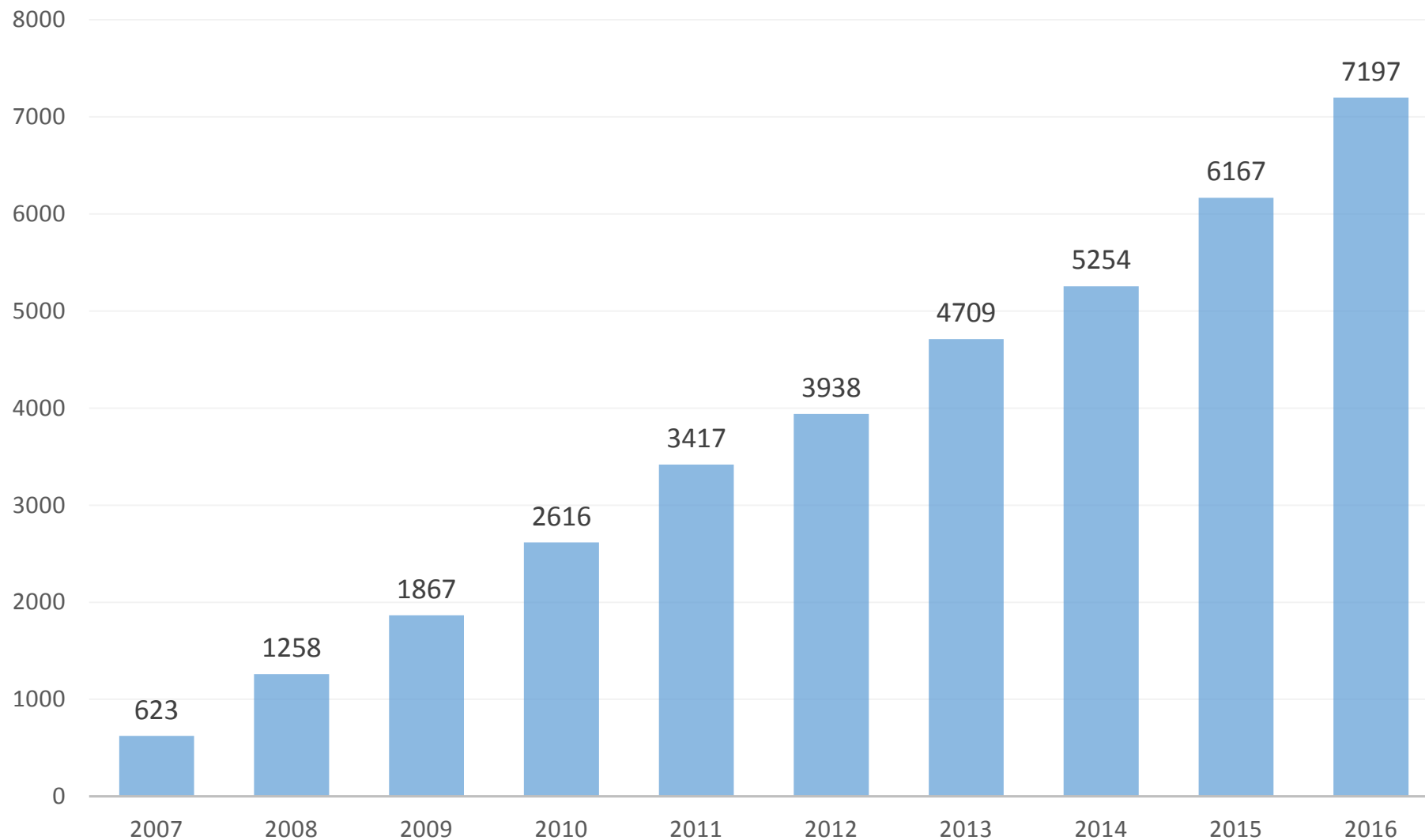
400 Guías generales	Publicado
CCN-STIC-426 REYES. Manual de usuario	Abr 2016

800 Guías Esquema Nacional de Seguridad	Publicado
CCN-STIC-809 Conformidad con el ENS	May 2016
CCN-STIC-817 Gestión de ciberincidentes en ENS	Jul 2016
CCN-STIC-824 Informe del Estado de Seguridad	Oct 2016
CCN-STIC-844 Manual de usuario de INES	Nov 2016
CCN-STIC-845A LUCIA. Manual de usuario	Abr 2016
CCN-STIC-845B LUCIA. Manual de usuario SAT	Feb 2016
CCN-STIC-845C LUCIA. Instalación	Nov 2016
CCN-STIC-845 D LUCIA. Administración	Nov 2016

2015: 23 nuevas guías
5 actualizadas

2016: 19 nuevas guías
12 actualizadas

Número de usuarios registrados en el portal, por año



➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

